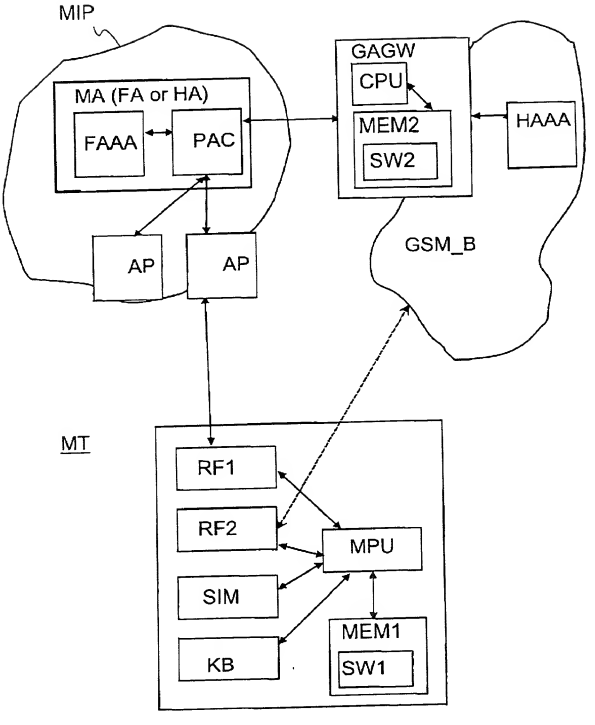
MIP
MA (FA or HA)
FAAA
PAC
AP
AP
GAGW
CPU
MEM2
SW2
HAAA
GSM_B
MT
RF1
RF2
MPU
SIM
KB
MEM1
SW1

Fig. 1

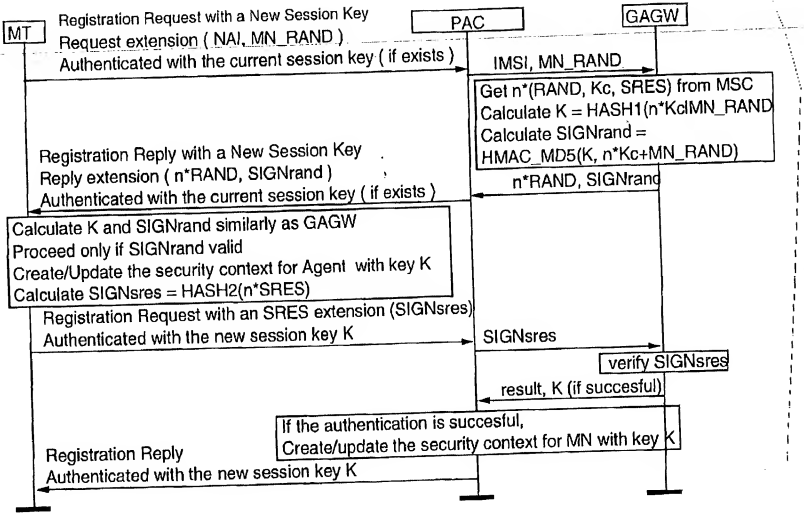
MT
PAC
GAGW
Registration Request with a New Session Key
Request extension (NAI, MN_RAND)
Authenticated with the current session key (if exists)
IMSI, MN_RAND
Get n*(RAND, Kc, SRES) from MSC
Calculate K = HASH1(n*Kc|MN_RAND
Calculate SIGNrand =
HMAC_MD5(K, n*Kc+MN_RAND)
Registration Reply with a New Session Key
Reply extension (n*RAND, SIGNrand)
Authenticated with the current session key (if exists)
n*RAND, SIGNrand
Calculate K and SIGNrand similarly as GAGW
Proceed only if SIGNrand valid
Create/Update the security context for Agent with key K
Calculate SIGNsres = HASH2(n*SRES)
Registration Request with an SRES extension (SIGNsres)
Authenticated with the new session key K
SIGNsres
verify SIGNsres
result, K (if succesful)
If the authentication is succesful,
Create/update the security context for MN with key K
Registration Reply
Authenticated with the new session key K

Fig. 2

T08OTO' 9LE9Z60

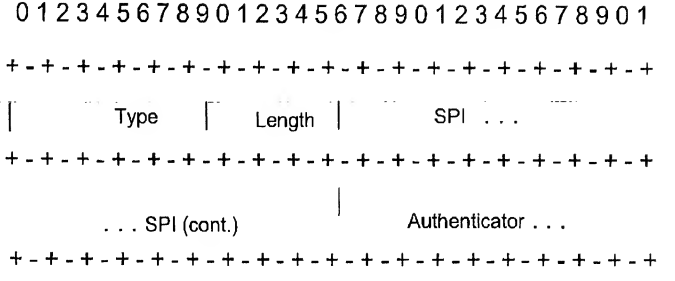

Fig. 3

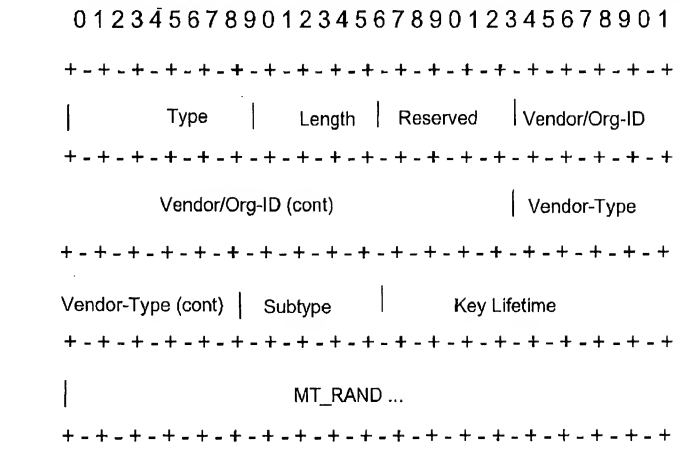
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Reserved
Vendor/Org-ID
Vendor/Org-ID (cont)
Vendor-Type
Vendor-Type (cont)
Subtype
Key Lifetime
MT_RAND ...

Fig. 4

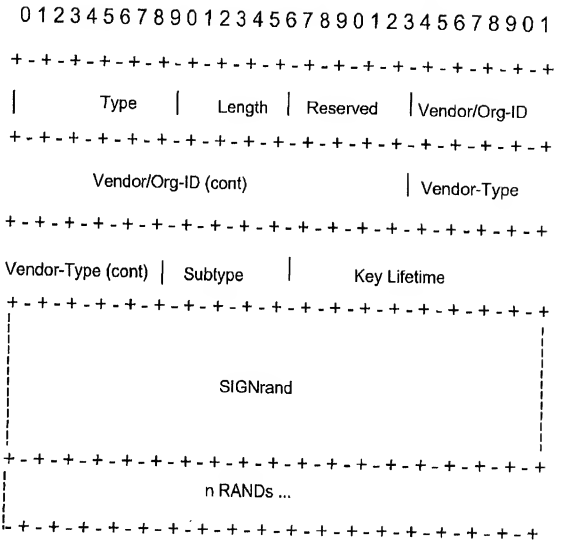
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Reserved
Vendor/Org-ID
Vendor/Org-ID (cont)
Vendor-Type
Vendor-Type (cont)
Subtype
Key Lifetime
SIGNrand
n RANDs ...

Fig. 5

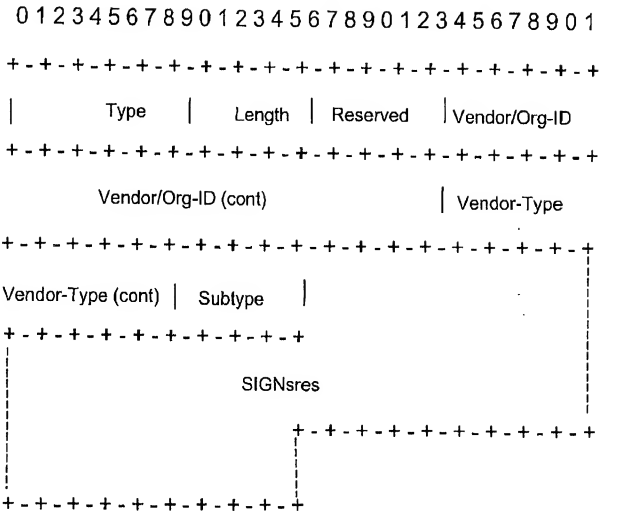
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Type
Length
Reserved
Vendor/Org-ID
Vendor/Org-ID (cont)
Vendor-Type
Vendor-Type (cont)
Subtype
SIGNsres

Fig.6

09/558,316 05/08/00

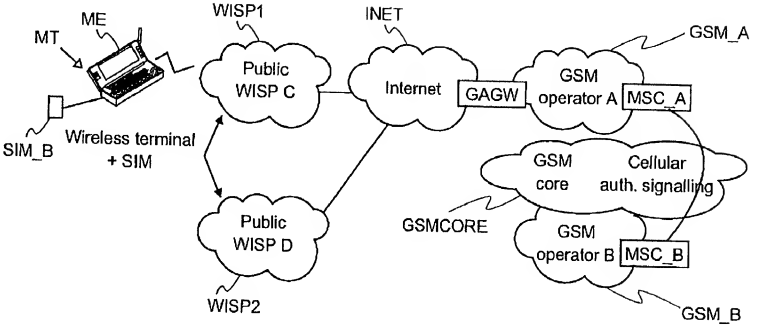

Fig. 7

TD80TO' SHE9SZ60

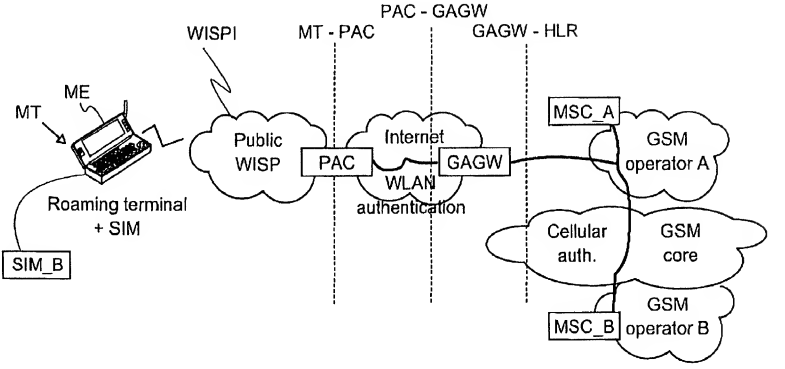

Fig. 8

T08070 S1eSSZ60

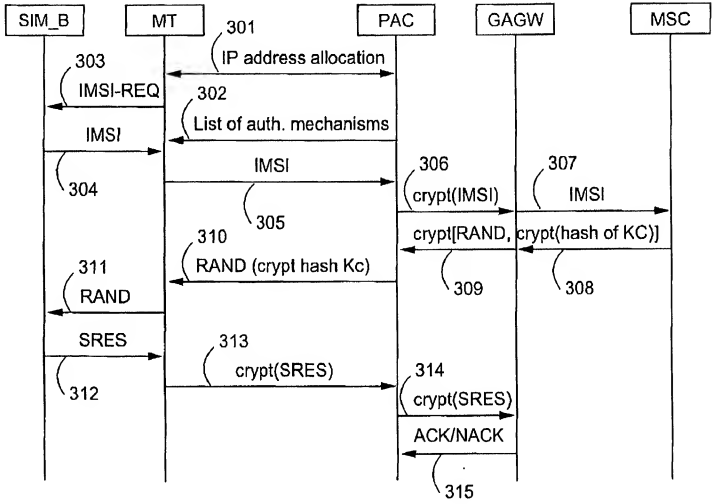

Fig. 9

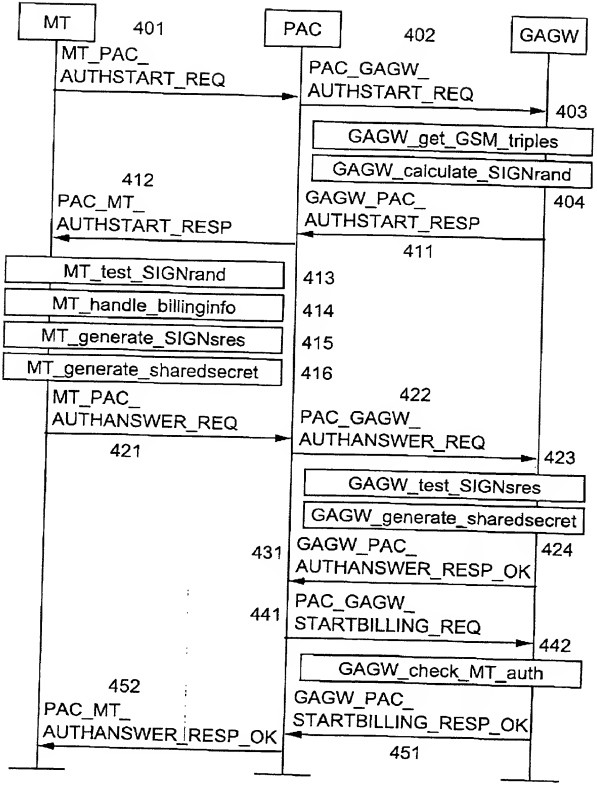
MT
401
PAC
402
GAGW
MT_PAC_
AUTHSTART_REQ
PAC_GAGW_
AUTHSTART_REQ
403
GAGW_get_GSM_triples
GAGW_calculate_SIGNrand
412
PAC_MT_
AUTHSTART_RESP
GAGW_PAC_
AUTHSTART_RESP
404
411
MT_test_SIGNrand
413
MT_handle_billinginfo
414
MT_generate_SIGNsres
415
MT_generate_sharedsecret
416
422
MT_PAC_
AUTHANSWER_REQ
PAC_GAGW_
AUTHANSWER_REQ
421
423
GAGW_test_SIGNsres
GAGW_generate_sharedsecret
431
GAGW_PAC_
AUTHANSWER_RESP_OK
424
441
PAC_GAGW_
STARTBILLING_REQ
442
GAGW_check_MT_auth
452
PAC_MT_
AUTHANSWER_RESP_OK
GAGW_PAC_
STARTBILLING_RESP_OK
451

Fig.10

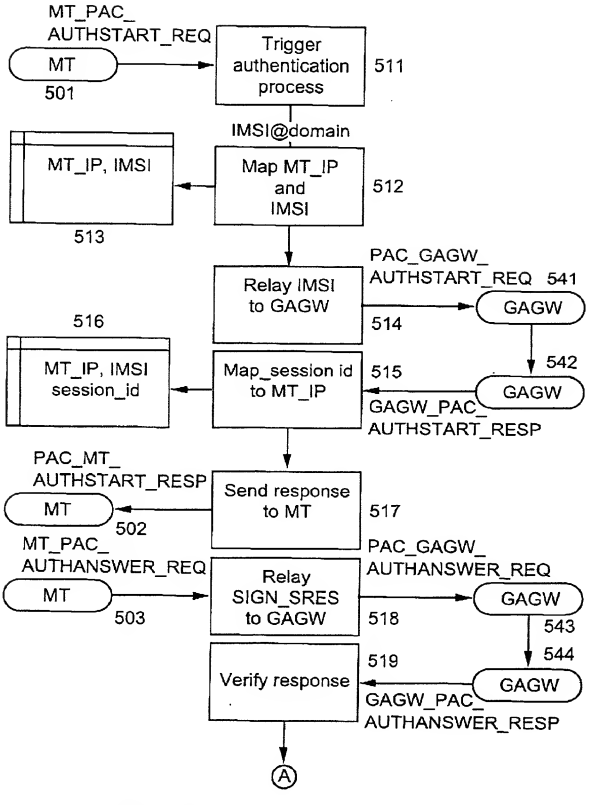
MT_PAC_
AUTHSTART_REQ
MT
501
Trigger
authentication
process
511
IMSI@domain
MT_IP, IMSI
513
Map MT_IP
and
IMSI
512
PAC_GAGW_
AUTHSTART_REQ
541
Relay IMSI
to GAGW
514
GAGW
542
516
MT_IP, IMSI
session_id
Map_session id
to MT_IP
515
GAGW
GAGW_PAC_
AUTHSTART_RESP
PAC_MT_
AUTHSTART_RESP
MT
502
Send response
to MT
517
MT_PAC_
AUTHANSWER_REQ
MT
503
Relay
SIGN_SRES
to GAGW
PAC_GAGW_
AUTHANSWER_REQ
518
GAGW
543
544
519
Verify response
GAGW
GAGW_PAC_
AUTHANSWER_RESP
A

Fig. 11a

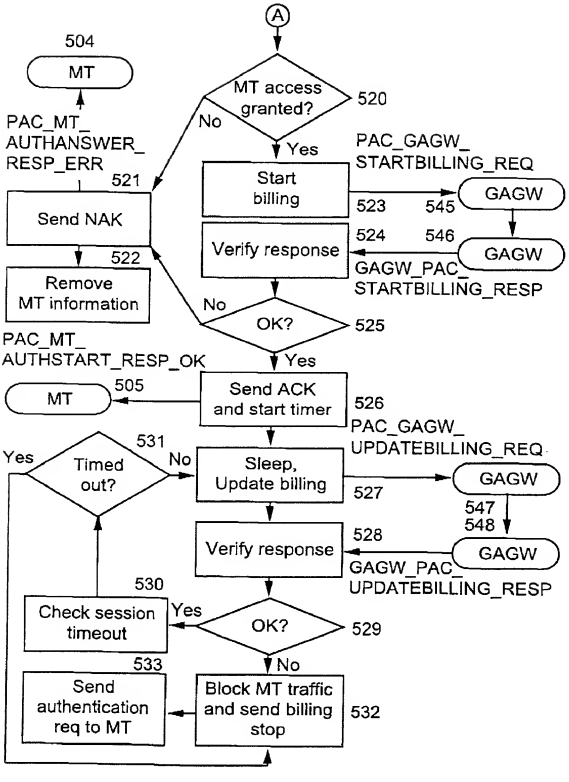
A
504
MT
PAC_MT_
AUTHANSWER_
RESP_ERR
521
Send NAK
522
Remove
MT information
MT access
granted?
520
No
Yes
PAC_GAGW_
STARTBILLING_REQ
Start
billing
523
545
GAGW
Verify response
524
546
GAGW
GAGW_PAC_
STARTBILLING_RESP
No
OK?
525
PAC_MT_
AUTHSTART_RESP_OK
Yes
MT
505
Send ACK
and start timer
526
PAC_GAGW_
UPDATEBILLING_REQ
Yes
531
Timed
out?
No
Sleep,
Update billing
527
GAGW
547
548
Verify response
528
GAGW
GAGW_PAC_
UPDATEBILLING_RESP
530
Check session
timeout
Yes
OK?
529
No
533
Send
authentication
req to MT
Block MT traffic
and send billing
stop
532

Fig. 11b

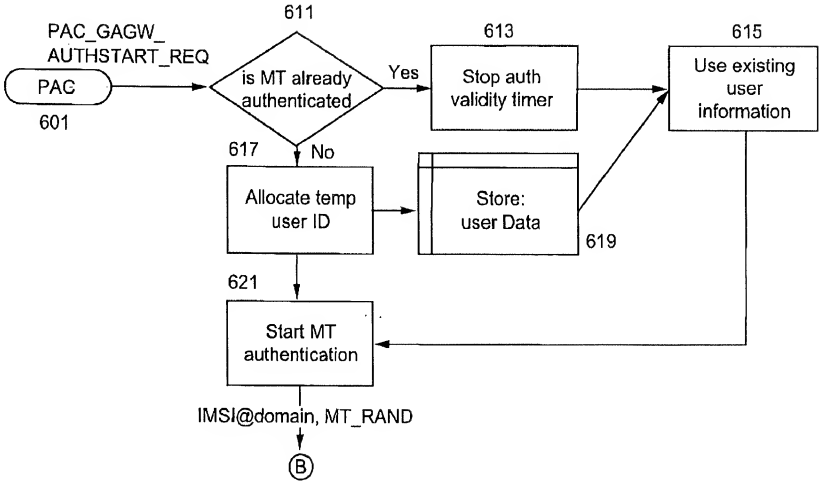
611
PAC_GAGW_
AUTHSTART_REQ
PAC
601
is MT already authenticated
Yes
613
Stop auth validity timer
615
Use existing user information
617
No
Allocate temp user ID
Store: user Data
619
621
Start MT authentication
IMSI@domain, MT_RAND
B

Fig. 12a

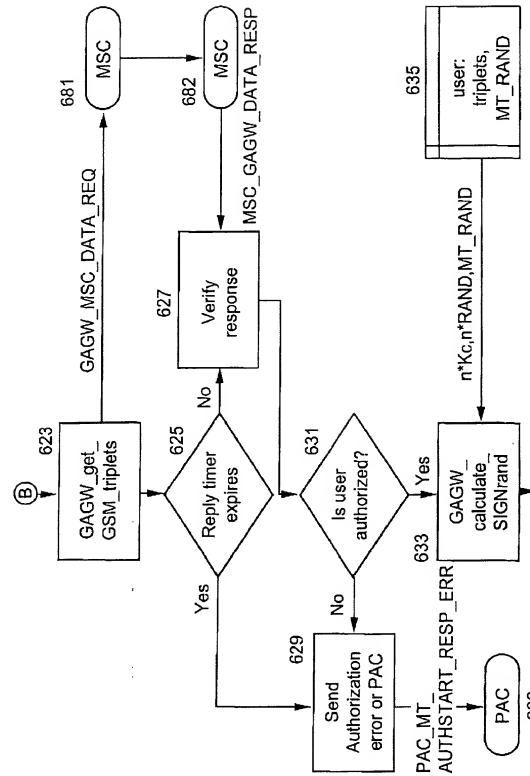
B
623
GAGW_get_GSM_triplets
GAGW_MSC_DATA_REQ
681
MSC
625
Reply timer expires
No
627
Verify response
682
MSC
MSC_GAGW_DATA_RESP
Yes
631
Is user authorized?
Yes
635
user: triplets, MT_RAND
n*Kc,n*RAND,MT_RAND
633
GAGW_ calculate_ SIGNrand
C
No
629
Send Authorization error or PAC
PAC_MT_ AUTHSTART_RESP_ERR
PAC
602

Fig. 12b

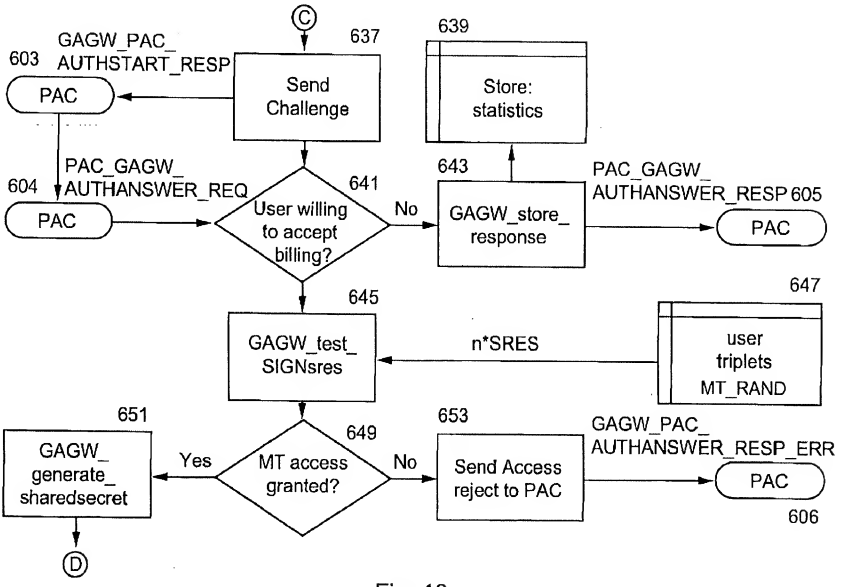
C
637
639
GAGW_PAC_
AUTHSTART_RESP
603
PAC
Send
Challenge
Store:
statistics
PAC_GAGW_
AUTHANSWER_REQ
604
PAC
641
User willing
to accept
billing?
No
643
GAGW_store_
response
PAC_GAGW_
AUTHANSWER_RESP 605
PAC
647
645
GAGW_test_
SIGNsres
n*SRES
user
triplets
MT_RAND
651
649
653
GAGW_
generate_
sharedsecret
Yes
MT access
granted?
No
Send Access
reject to PAC
GAGW_PAC_
AUTHANSWER_RESP_ERR
PAC
606
D

Fig. 12c

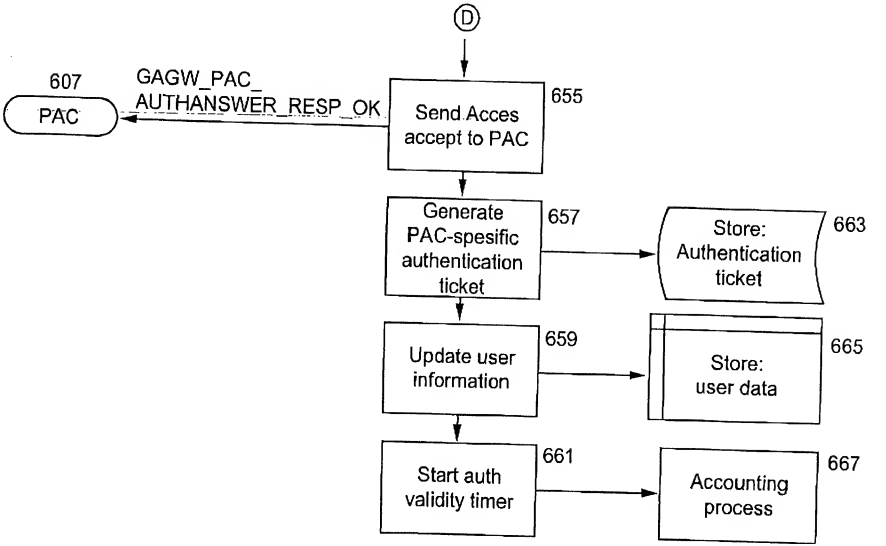
D
607
PAC
GAGW_PAC_
AUTHANSWER_RESP_OK
Send Acces
accept to PAC
655
Generate
PAC-spesific
authentication
ticket
657
Store:
Authentication
ticket
663
Update user
information
659
Store:
user data
665
Start auth
validity timer
661
Accounting
process
667

Fig. 12d

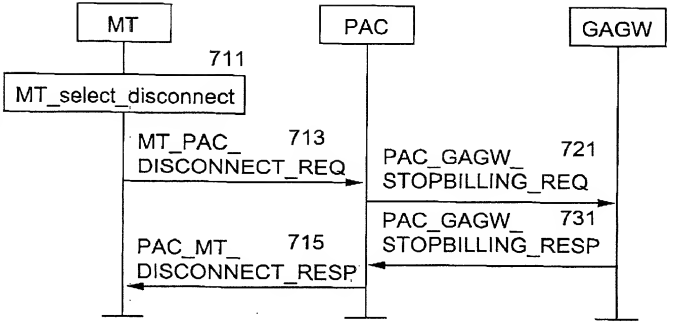
MT
PAC
GAGW
711
MT_select_disconnect
MT_PAC_ 713
DISCONNECT_REQ
PAC_GAGW_ 721
STOPBILLING_REQ
PAC_GAGW_ 731
STOPBILLING_RESP
PAC_MT_ 715
DISCONNECT_RESP

Fig. 13

#	MT	PAC	GAGW
(1)	HDR, SA, KE [, CERTREQ] =>		
(2)		<= HDR, SA, KE [, CERT_GAGW]	
(3)	HDR*, IDmt, Nmt =>		
(4)			IMSI, MT_RAND=>
(5)			<= n*RAND, SIGNrand, MT_RAND, billingInfo
(6)		<= HDR*, Npac, HASH(1), NOTIFY	
(7)	HDR*, HASH(2) =>		
(8)			SIGNsres, MT_RAND=>
(9)			<= SIGNresult, MT_RAND, sessiontimeout, Kpac_MT
(10)		<= HDR*, <SA_b>KpacMT, HASH(3)	

Fig. 14

#	MT	PAC
(1)		<= HDR, SA
(2)	HDR, SA, KE [, CERTREQ] =>	
(3)		<= HDR, KE [, CERT_GAGW]

Fig. 15

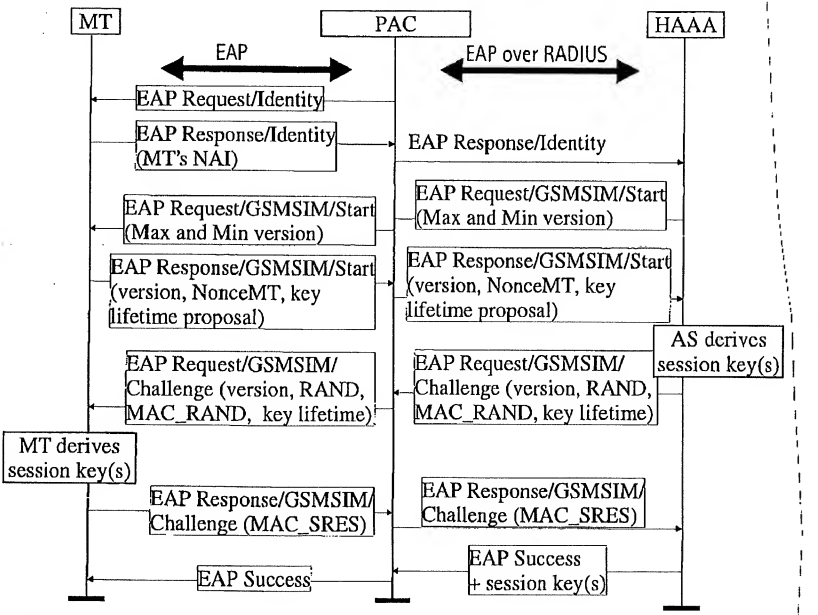
MT
PAC
HAAA
EAP
EAP over RADIUS
EAP Request/Identity
EAP Response/Identity (MT's NAI)
EAP Response/Identity
EAP Request/GSMSIM/Start (Max and Min version)
EAP Request/GSMSIM/Start (Max and Min version)
EAP Response/GSMSIM/Start (version, NonceMT, key lifetime proposal)
EAP Response/GSMSIM/Start (version, NonceMT, key lifetime proposal)
AS derives session key(s)
EAP Request/GSMSIM/ Challenge (version, RAND, MAC_RAND, key lifetime)
EAP Request/GSMSIM/ Challenge (version, RAND, MAC_RAND, key lifetime)
MT derives session key(s)
EAP Response/GSMSIM/ Challenge (MAC_SRES)
EAP Response/GSMSIM/ Challenge (MAC_SRES)
EAP Success
EAP Success + session key(s)

Fig. 16